Architectural Issues with the Use of IPSec

ICNS 2004

Ruben Bigio, FAA
Simon Blake-Wilson, BCI
Jamie Chappell, BCI
Luoping Liu, BCI
Vic Patel, FAA ACB-250
Jim Simpkins, BCI

Outline

- Motivation
- IPSec overview
- Cryptographic algorithms for IPSec
- IPSec and IPv6
- Demonstration of IPSec within the NAS
- Conclusions

Motivation

This presentation reports on a study performed by FAA ACB-250 in support of ASD-130 considering the security issues that will arise as TCP/IP is deployed within the NAS.

Motivation (cont)

A number of “unique” characteristics of the NAS and aeronautical networks in general must be considered:

- Safety critical
- Certification requirements
- Scalability
- Latency
- Reliability
- Interoperability
- Support for air/ground connections
- Transition from legacy networking technologies
- Desire to transition to IPv6

IPSec Overview

IPSec is the network layer security standard in the TCP/IP protocol stack. It is widely used to secure site-to-site and remote access connections.

IPSec consists of three protocols:

- Internet Key Exchange - IKE
- Authentication Header - AH
- Encapsulated Security Payload - ESP

AH and ESP operate in Transport or Tunnel mode.

IPSec Overview – Transport Mode

Transport Mode:

- Used between 2 end systems (hosts)
- Originating source and IPSec processing source are the same
- IPSec processing destination and ultimate destination are the same
- Additional protocol header added to IP packet

IPSec Overview – Tunnel Mode

Tunnel Mode:

- Used between 2 security gateways, or routers
- Used between an end system and security gateway in typical remote access scenario
- Originating source and IPSec processing source may be the same or different
- IPSec processing destination and ultimate destination may be the same or different
- Encapsulates original IP packet
- Outer IP header contains IPsec processing end points
- Inner IP header contains originating source and ultimate destination

Crypto Algorithms for IPSec

Goal: Recommendations for cryptographic algorithms to be purchased and used with IPSec

Issues:

- Security – default IPSec algorithm is not secure
- Interoperability – boxes that do not support common algorithms cannot talk to each other
- Also relevant in ATN where boundary equipment between States will need to use common algorithms

Crypto Algorithms for IPSec – Security Levels

Primary desire is security. Suitable security levels:

Source	80 bits	112 bits	128 bits
Lenstra	2013	2050 (109 bits)	
RSA Security	2010	2030	2031+
NIST	2015	2035	2036+

Crypto Algorithms for IPSec – NIST Compliance

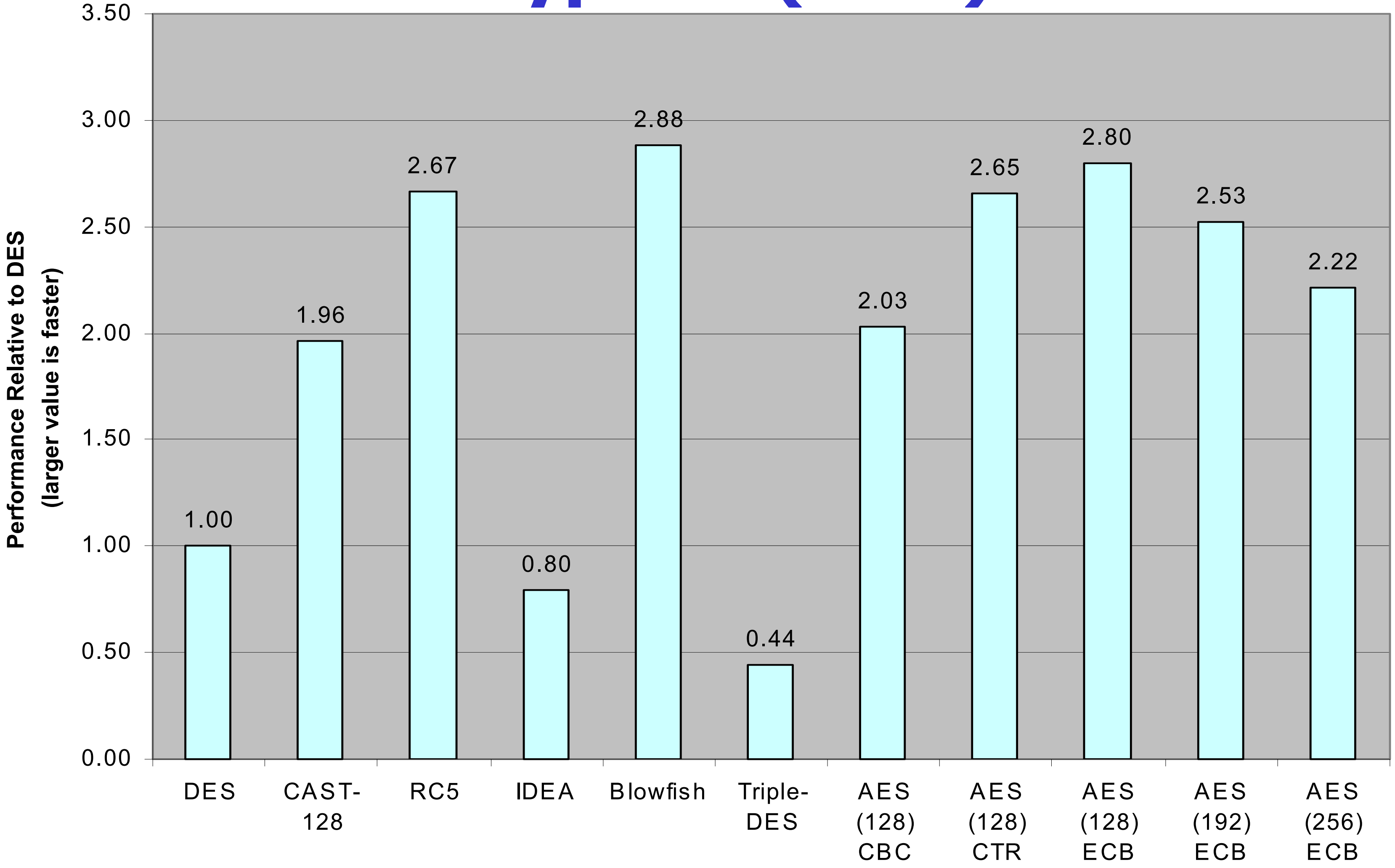
US Government is also required to comply with NIST standards:

- FIPS 46-3 – DES and Triple DES
- FIPS 180-2 – SHA-1, SHA-256, SHA-384, SHA-512
- FIPS 197 – AES
- FIPS 198 – HMAC
- SP 800-38A – Modes of operation
- SP 800-38C – Additional CCM mode

Crypto Algorithms for IPSec - Encryption

- IPSec mandates the support of the following symmetric encryption algorithms in all IPSec implementations
  - –DES in CBC mode, NULL encryption algorithm (i.e., no encryption)
- IPSec allows the support of the following in CBC mode
  - –CAST-128, RC5, IDEA, Blowfish, Triple-DES, AES
- AES-CTR and AES-CCM are specified in IETF Internet Drafts
- AES will become the default symmetric encryption algorithm for IPSec

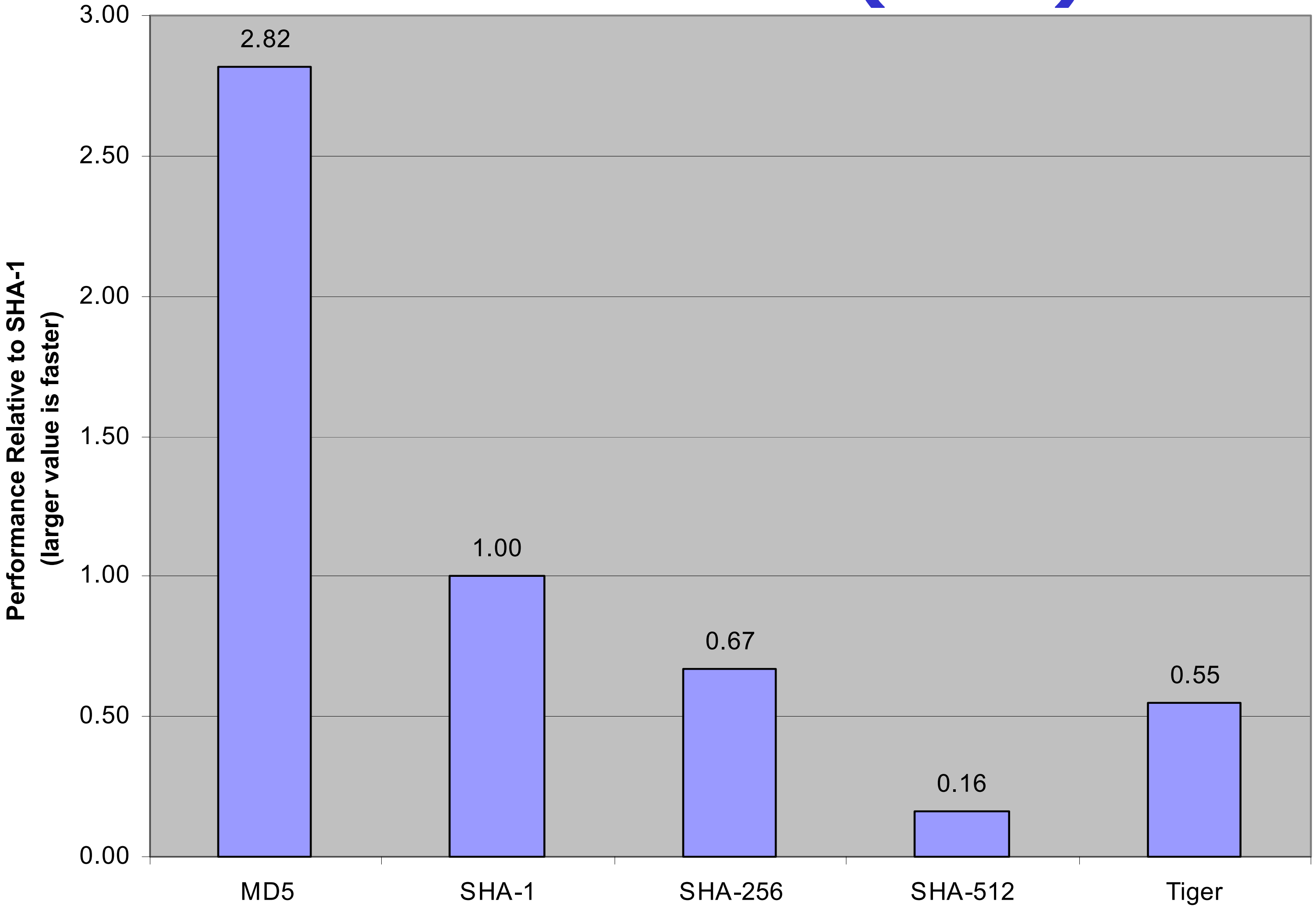
Crypto Algorithms for IPSec – Encryption (cont)



Crypto Algorithms for IPSec - Authentication

- IPSec mandates the support of the following symmetric authentication algorithms in all IPSec implementations
  - –HMAC-MD5-96, HMAC-SHA-1-96, NULL authentication algorithm (i.e., no authentication)
- IPSec allows the support of the following
  - –HMAC with Tiger (IKE only), HMAC-RIPEMD-160-96, AES-XCBC-MAC-96

Crypto Algorithms for IPSec – Authentication (cont)



Crypto Algorithms for IPSec - Recommendations

- Purchase only implementations that have support for AES with 128-bit keys, Triple-DES, and HMAC-SHA-1-96
  - *Be careful!* Some vendors support AES in ESP but not IKE
- Use AES with 128-bit keys and HMAC-SHA-1-96
  - Triple-DES should be used only as a fallback for systems that cannot support AES
- Refuse to negotiate the use of all other symmetric encryption and authentication algorithms (e.g., DES, HMAC-MD5-96)
- These recommendations apply to any IPSec deployment, including the use of IPSec to secure ATN traffic

IPSec and IPv6

What: Investigation of benefits and issues associated with the use of IPSec with IPv6

- Benefits:
  - –IPSec mandatory in IPv6
  - –Talk of end-to-end IPSec
  - –Less need for NAT
- Issues
  - –IPSec and migration from IPv4 and IPv6
  - –End-to-end IPSec, packet filtering, and net management

IPSec and IPv6 – End-to-End IPSec

- Packet-filtering. e.g. at the firewall, is made more difficult and thus end-to-end IPSec may have to be disallowed by corporate firewall configurations. Firewall vendors are wrestling with this issue
- Network management faces increased challenges as encrypted packets may limit its functionality.

IPSec and IPv6 – End-to-End IPSec (cont)

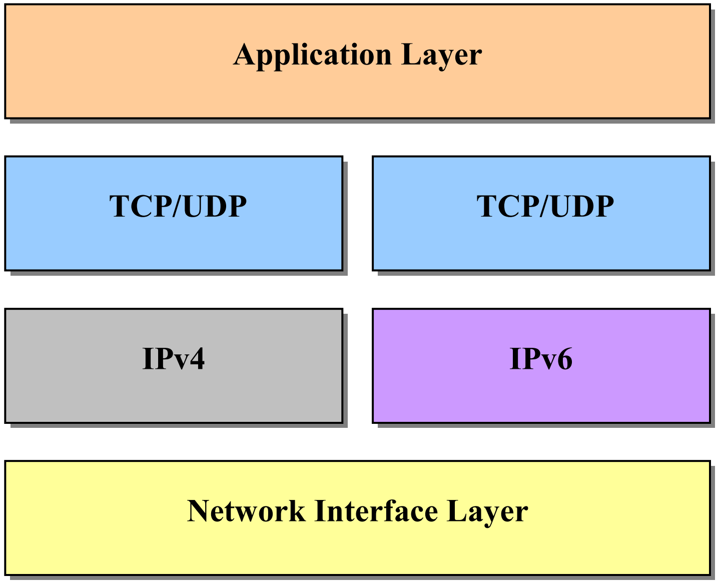
- Larger numbers of devices using IPSec will increase key management problems
- Pre-shared key - the most widely used form of credentials – already suffers from security problems
- PKI may provide a solution

IPSec and IPv6 – End-to-End IPSec (cont)

- Interoperability is an existing problem for IPSec
- Less need for NAT in IPv6 will help
- But NAT will still be needed to hide network topology of private networks
- More vendors implementing IPSec since it is mandatory will increase problems
- A lot of the interoperability problems with IPSec are due to vagaries of IKE specification – IKEv2 may help

IPSec and IPv6 – Migration – Dual Stack

IPv4 to IPv6 migration almost always involves a dual stack machine, whether end system or intermediate system.



Such dual stack machines are susceptible to both IPv4-based vulnerabilities, and IPv6 vulnerabilities

IPSec and IPv6 – Migration – Tunneling

Tunneling refers to the encapsulation of an IPv6 packet inside an IPv4 packet to enable the packet to traverse a network that has not been upgraded.

There are a large number of techniques: configured tunnels, automatic tunnels, 6to4, 6over4, Teredo, etc.

Fundamental problem: an IPSec tunnel cannot start outside the tunnel and end inside the tunnel – therefore location of IPSec endpoints must be taken into account.

IPSec and IPv6 – Migration – Translation

Translation offers a means to translate an IPv4 header into an IPv6 header in order to allow applications to communicate in a mixed protocol environment.

There are a large number of techniques: stateless IP / ICMP translation algorithm, bump-in-the-stack, bump-in-the-API, transport relay translator.

Problems differ. For example, stateless IP/ICMP is incompatible with AH, and ESP in tunnel mode.

IPSec Demonstration

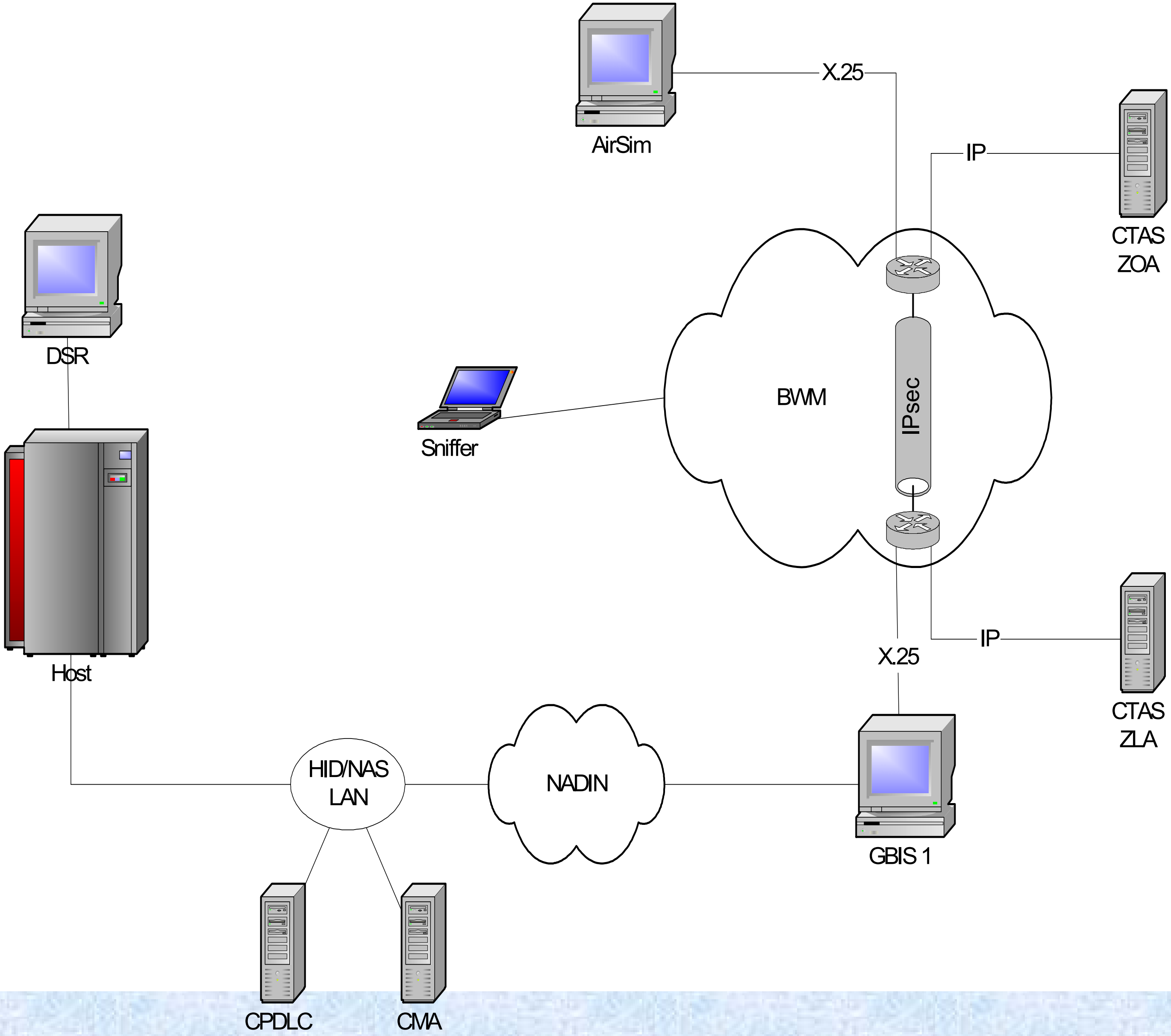
What: Show IPSec deployed in a “good” configuration within NAS applications

- Provides a concrete example
- CPDLC over TCP/IP!
- Shows the benefits of “good” IPSec deployment within system architecture

IPSec Demonstration (cont)

- CPDLC and CTAS used as demo applications
- CPDLC with TCP/IP subnetwork (using XOT for now)
- BWM network infrastructure
- Centralized IPSec

IPSec Demonstration (cont)



Conclusions

- Standards like IPSec can be used to make TCP/IP networks at least as secure as legacy networks
- In an aeronautical environment, deployment of TCP/IP should take security into account
- Careful planning required to ensure interoperability, transition from IPv4 to IPv6, etc when using IPSec
- A number of areas where more work is needed:
    - IPSec credentials
    - IPSec reliability
    - Performance in NAS environment